UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/599,124	06/22/2000	Randy Eye	1999-31	7362

23823 7590 06/23/2004

Digital Video Express, LP
1408 BAYSHIRE LANE
Herndon, VA 20170

EXAMINER	
MCARDLE, JOSEPH M	
ART UNIT	PAPER NUMBER
2132	5

DATE MAILED: 06/23/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	**Application No.** 09/599,124	**Applicant(s)** EYE ET AL.
	Examiner Joseph McArdle	**Art Unit** 2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 June 2000*.

2a)□ This action is **FINAL**. 2b)☒ This action is non-final.

3)□ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-32* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)□ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-32* is/are rejected.

7)□ Claim(s) _____ is/are objected to.

8)□ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)□ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *6-22-2000* is/are: a)□ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)□ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)□ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)□ All b)□ Some * c)□ None of:

1.□ Certified copies of the priority documents have been received.

2.□ Certified copies of the priority documents have been received in Application No. _____.

3.□ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)

2) □ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 4.

4) □ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) □ Notice of Informal Patent Application (PTO-152)

6) □ Other: _____.

DETAILED ACTION

Drawings

1. The drawings are objected to because part of them are hand written. Corrected drawing sheets are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. The figure or figure number of an amended drawing should not be labeled as "amended." If a drawing figure is to be canceled, the appropriate figure must be removed from the replacement sheet, and where necessary, the remaining figures must be renumbered and appropriate changes made to the brief description of the several views of the drawings for consistency. Additional replacement sheets may be necessary to show the renumbering of the remaining figures. The replacement sheet(s) should be labeled "Replacement Sheet" in the page header (as per 37 CFR 1.84(c)) so as not to obstruct any portion of the drawing figures. If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Claim Objections

2. Claims 1 and 19 are objected to because of the following informalities: Claim 1 recites "with a key registers". The examiner asserts that this should read as "with a key

register". Claim 19 recites "an data type. The examiner asserts that this should read "a data type". Appropriate correction is required.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-8, 10-25, and 26-32 are rejected under 35 U.S.C. 102(e) as being anticipated by Ober (U.S. Patent No. 6307936). In regards to claim 1, Ober discloses a design that pertains to a cryptographic management scheme. Ober further discloses in column 12, lines 29-30 that keys are stored in key cache registers (KCRs). This disclosure meets the limitations set forth under claim 1 that call for have a multitude of key registers. Ober then discloses in column 12, lines 35-67 through column 13, lines 1-24 that the storage format of the keys in the KCRs includes numerous fields that indicate things such as the type of key, length of the key, etc. This disclosure meets the limitations set forth under claim 1 that call for having a multitude of type fields associated with a key register. Ober then discloses in column 8, lines 28-34 that a key management scheme referred to as "CryptIC" is responsible for controlling and performing various key management functions and algorithms. This disclosure meets

the remaining limitations set forth under claim 1 that call for having a key management controller (CryptIC), key management algorithms and key management functions.

5. In regards to claim 19, Ober discloses a design that pertains to a cryptographic management scheme. Ober further discloses in column 12, lines 29-30 that keys are stored in key cache registers (KCRs). Ober then discloses that two types of keys that are employed by the management scheme (see column 3, lines 1-16). These two key types are data keys (DK), which are used to encrypt data, and key encryption keys (KK), which are used to allow for the secure distribution of keys by encrypting other keys with them. Ober then discloses in column 12, lines 35-67 through column 13, lines 1-24 that the storage format of the keys in the KCRs includes numerous fields that indicate things such as the type of key, length of the key, etc. These disclosures meet the limitations set forth under claim 19, which call for storing data keys and key keys (key encryption keys) in a key register along with their associated types in a key field and for using a key register to perform a key management function.

6. In regards to claims 2 and 20, Ober discloses in column 3, lines 1-16 that data keys (DK) and key encryption keys (KK) are used in the key management scheme. Ober then discloses in column 12 lines 29-30 that keys (such as DK and KK) are stored in KCRs. Ober then discloses in column 12, lines 35-67 through column 13, lines 1-24 that the storage format of the keys in the KCRs includes numerous fields that indicate things such as the type of key, length of the key, etc. These disclosures meet the limitations set forth under claims 2 and 20 that call for allowing a key type field to have values including at least one of KK, DK, and NULL.

7. In regards to claim 3, Ober discloses in column 3, lines 1-16 that key encryption keys (KK) are used to encrypt other keys such as data keys (DK). This disclosure meets the limitations set forth under claim 3 that call for having a KK for encrypting/decrypting the contents of other key registers.

8. In regards to claims 4 and 21, Ober discloses in column 10, lines 56-62 that decrypting key encryption keys (DKEKs) are used to wrap and unwrap data encryption keys (DK). It is further disclosed in the aforementioned location that the DKEK type keys are used to uncover (unwrap) "black" DEKs (encrypted data encryption keys). These disclosures meet the limitations set forth under claims 4 and 21 that call for having wrapped key parameters for specifying an unwrapping key (DKEK tye keys are used to unwrap "black DEK type keys), a type parameter for specifying an unwrapping key type (DKEK type key), and a wrapped key parameter indicating a wrapped key ("black" DEK key types). Ober further discloses in the aforementioned location that "black" DEK type keys can be stored in a crypto context database. This disclosure meets the limitations set forth under claims 4 and 21 that call for having a parameter that specifies where to store the unwrapped key ("black" DEKs get stored in a crypto context database).

9. In regards to claims 5 and 22, Ober further discloses in column 10, lines 10-15 that key encryption keys (KK) allow for the covering (wrapping) of other keys. The key encryption keys are capable of encrypting other keys (such as data encryption keys) so they can be securely exchanged. This disclosure meets the limitations set forth under claims 5 and 22 that call for having a wrapping key parameter for specifying a wrapping

key to allow the wrapping of the wrapping key using the wrapping key key (KK) because Ober's key encryption key (KEK) is used to wrap other keys with such parameters as a data encryption key (DEK).

10. In regards to claims 6, 7, 23, and 24, Ober discloses in column 6, lines 13-16 that the type of key specifies what key an algorithm can be used in. The use of the term algorithm in this case refers to what algorithm can be used for encryption and decryption of data. (i.e. DES, 3DES, RSA). In other words, if the data is to be encrypted according to a particular key then that key dictates what type of encryption algorithm is to be used. The same holds for decrypting data as well, in that if the data was encrypted according to a particular algorithm then an appropriate decryption key must be indicated. These disclosures meet the limitations set forth under claims 6, 7, 23, and 24 that call for encrypting and decrypting data based on a key index parameter specifying an encryption/decryption key (the parameter in the present case can identify what type of key it is and its associated decryption/encryption algorithm).

11. In regards to claims 8 and 25, Ober discloses in column 3, lines 34-35 and 44-45 that symmetrical key generation can be performed six ways and that one such was is to import a RED (plaintext) key. Ober further discloses in column 9, lines 61-65 that data encryption keys can be imported as a RED key. This disclosure meets the limitations set forth under claims 8 and 25 that call for loading a plaintext key into a key register specified by an index parameter because the storage destination can be indicated by what type of key it is (i.e. a data encryption key, key encryption key, etc).

12. In regards to claims 10 and 27, Ober discloses in column 10, lines 6-8 that upon a reset all volatile key cache locations (KCRs) will be cleared. This disclosure meets the limitations set forth under claims 10 and 27 that call for having an initialization function to clear a multitude of key registers because upon start up (initializing) the key cache registers will be cleared. Ober further discloses in column 12, lines 29-30 that keys are stored in key cache registers (KCRs). Ober then discloses in column 12, lines 35-67 through column 13, lines 1-24 that the storage format of the keys in the KCRs includes numerous fields that indicate things such as the type of key, length of the key, etc. Ober then discloses in column 16, lines 15-21 that an application can import (to a KCR) its own RED keys (plaintext == RED) to be used as key encryption keys (KK). These disclosures meet the limitations set forth under claims 10 and 27 that call for storing a plaintext key in a register and storing a KK value in the type field because in Ober's disclosure, if a RED key is imported for the purposes of using it as a key encryption key, the type field will indicate it as a key encryption key.

13. In regards to claims 11 an 28, Ober discloses in figure 4 a tree hierarchy that is used in the key management scheme. This disclosure meets the exact limitations set forth under claims 11 and 28.

14. In regards to claims 12 and 29, Ober discloses a hierarchy in figure 2 that depicts how keys can only cover (wrap) keys of a lower level. This disclosure meets the exact limitations set forth under claims 12 and 29.

15. In regards to claims 13 and 30, Ober's design mentioned above discloses hoe key cache registers contain a root key and that there is a multitude of key cache

registers therefore allowing for multiple root keys. This disclosure meets the limitations set forth under claims 13 and 30 that call for having more than 1 root key.

16. In regards to claims 14 and 31, Ober discloses in column 6, lines 13-16 that the type of key specifies what key the algorithm can be used in. The use of the term algorithm in this case refers to what algorithm the key management scheme will use for encryption and decryption. This disclosure meets the limitations set forth under claims 14 and 31 that call for using a key management algorithm determined by the value stored in the type field because in Ober's design, different encryption algorithms can be employed depending on the type of key in the key cache register (KCR).

17. In regards to claims 15 and 32, Ober discloses in column 3, lines 10-16 that key encryption keys can be used in order to allow for key distribution. Ober further discloses in column 4, lines 14-23 that a public key scheme can be used to import and export keys from the previously described management scheme. These disclosures meet the limitations set forth under claims 15 and 32 that call for using public key negotiation protocols to share keys with other management apparatuses.

18. In regards to claims 16 and 17, Ober discloses in column 10, lines 27-28 that key encryption keys (KEKs) are used to cover other KEKs and data encryption keys (DEKs). This allows for a DEK to be covered (wrapped) by a KEK. Ober further discloses in column 10, lines 25-26 that if a KEK is to be off loaded it gets covered by another encryption key. This is directly comparable to wrapping a data encryption key with a key encryption key and then wrapping that with the key encryption key again.

Therefore, this disclosure meets the limitations set forth under claims 16 and 17 where the wrapped data key (DK) = Ekk(Ekk(DK)).

19. In regards to claim 18, It has been previously described how the key management scheme employs the use of various encryption and decryption algorithms. One such algorithm is the DES algorithm, which uses bit wise XORing. This disclosure meets the exact limitations set forth under claim 18.

Claim Rejections - 35 USC § 103

20. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

21. Claims 9 and 26 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ober in view of Matyas (U.S. Patent No. 4941176). In regards to claim 9, Ober's design disclosed above meets all of the aforementioned limitations set forth under claim 1. However Ober's design makes no mention of providing a register clear function that is capable of clearing a specific key register and its associated fields. Matyas discloses a design relating to key management and describes in column 68, lines 10-39 a function that is responsible for clearing a key from a key register. It would have been obvious to one of ordinary skill in the art at the time the invention was made to combine Matyas's teachings on having a clear register function into Ober's design in order to create a design that is capable of clearing a key along with the key type field from a register

Conclusion

22. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. - Matyas (U.S. Patent No. 5142578) -

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Joseph McArdle whose telephone number is (703) 305-7515. The examiner can normally be reached on Weekdays from 8:00 am - 5:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on (703) 305-1830. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

JMM

Joseph McArdle
Examiner
Art Unit 2132

jmm

Gilberto Barron

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100